

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

OCTOBER 1976

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

Classified by DIRNSA/CHCSS (NSA/CSSM-123-2)
Exempt from GDS, EO 11652, Category 2
Declassify Upon Notification by the Originator

~~TOP SECRET~~

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,
for the Personnel of Operations

VOL. III, No. 10OCTOBER 1976

PUBLISHER

WILLIAM LUTWINIAK

BOARD OF EDITORS

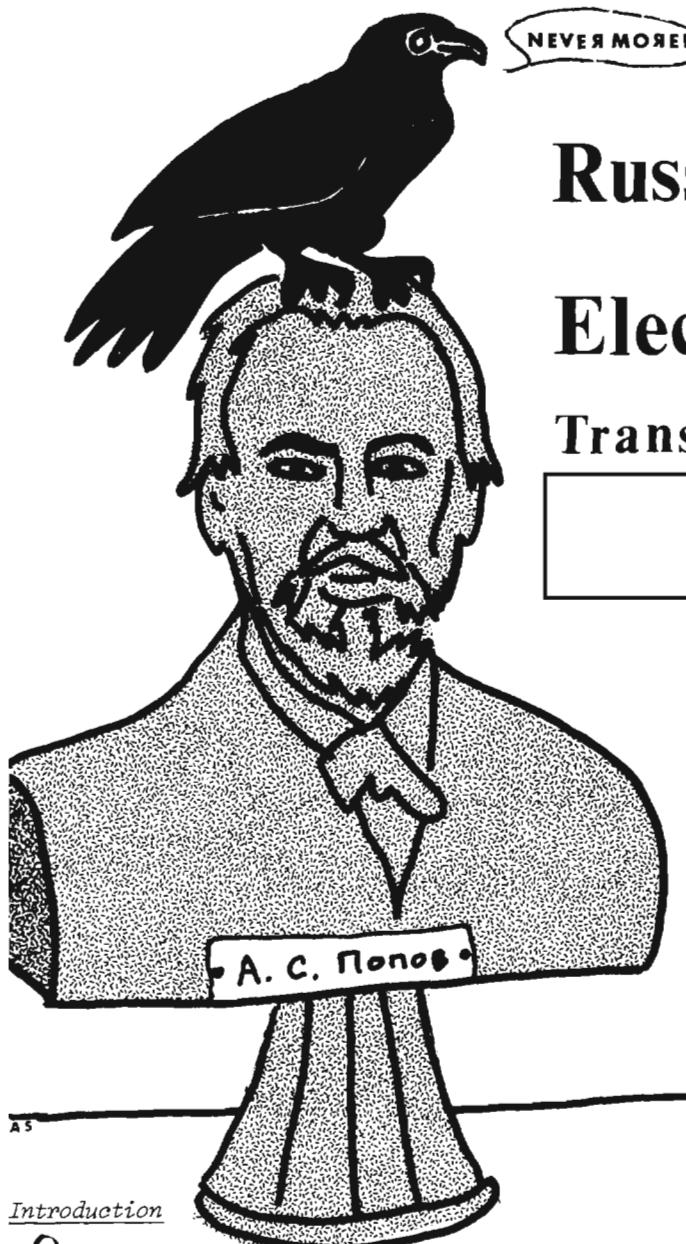
Editor in Chief.....Arthur J. Salemme (5642s)
Collection.....[redacted] (8955s)
Cryptanalysis.....[redacted] (8025s) P.L. 86-36
Language.....Emery W. Tetrault (5236s)
Machine Support.....[redacted] (3321s)
Mathematics.....Reed Dawson (3957s)
Special Research.....Vera R. Filby (7119s)
Traffic Analysis.....Frederic O. Mason, Jr. (4142s)

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

~~TOP SECRET~~

UNCLASSIFIED

P.L. 86-36

Introduction

Since approximately the 1940's, the struggle against electromagnetic emanations "in the ether" has been called the "radioelectronic struggle," or, to use U.S. terminology, "electronic warfare."

By "radioelectronic struggle" one understands the acquiring of intelligence on the enemy's radio-electronic means, the neutralization of their operation by the use of special emanations (jamming); the feeding of misinformation to the enemy; and the protection of friendly radioelectronic systems and methods against the enemy's intelligence and neutralization operations.

Pre-World War I Developments

The concepts of the radioelectronic struggle were expressed by the inventor of radio, the

Russian SIGINT & Electronic Warfare

Translated by

Translator's note: The reluctance on the part of the Soviets to discuss their own activities in the areas of intelligence-gathering and electronic warfare will come as no surprise to the reader. Recently, however, the Soviets have tried to document, at least superficially in open sources, some of their activities in these two sensitive areas.

The following is a translation of an article appearing in Voenno-istoricheskiy zhurnal (Journal of Military History), No. 3, 1975, entitled "From the History of Radioelectronic Warfare." The authors, General-Major of Communications Troops V. Grankin and Colonel V. Zmievskij, discuss the evolution of Soviet SIGINT and electronic warfare from a historical point of view. Although the article is somewhat sketchy, the authors do cite Ministry of Defense Archives as the sources of some of their information. The most important point stressed by the authors is the total integration of SIGINT with electronic warfare.

I have taken the liberty of deleting two sections -- one section pertaining to Lenin's views on radio as a propaganda instrument, and the other pertaining to the role played by non-Soviet (i.e. German, U.S., etc.) SIGINT/EW in World War II, since only well-known Western sources are cited. The deletion of these two sections takes nothing away from the main thrust of the article.

UNCLASSIFIED

UNCLASSIFIED

Russian scientist A. S. Popov. In a memorandum dated 17 March 1903 to the Russian War Department concerning the establishment of radio communications between Varna and Odessa, A. S. Popov noted that it would be preferable to run the radio line not directly from Varna to Odessa, but from Varna to Sevastopol' to Odessa. That would allow the radio line to be farther away from the Romanian shores, thus making it almost impossible for anyone to monitor its operation or to interrupt its operation with the use of electromagnetic waves. As we can see, the idea of the possible conducting of intelligence and the creation of radio jamming was expressed for the first time by the inventor of radio himself, and it was he who proposed measures to protect radio communications from intelligence-gathering and neutralization operations.

The first attempts at conducting radio-electronic suppression operations, i.e. the use of electromagnetic energy as a kind of "weapon" against electronic systems, occurred during the Russo-Japanese War.

It is a well-known historical fact that in 1905, in the Tsushima Strait area, the Japanese light cruiser Izumi, which was proceeding along a course parallel to that of a squadron of Russian ships, informed its headquarters by radio concerning the number of ships in the squadron. The commander of the Russian cruiser Ural, having detected the Japanese radio transmissions, decided to suppress them by using the radio set on board his ship. This was reported to the Squadron Commander-in-Chief, Admiral Rozhestvenskij, who, incidentally, had categorically forbidden taking such action. Nevertheless, the commanders of the cruiser Izumrud and the torpedo boat Gromkij, on their own initiative, used their shipboard radio sets to suppress the radio communications of the Japanese naval vessels. Thus, measures to suppress an enemy's radio-communications system were carried out for the first time by Russian military specialists.

World War I

During World War I, an organized struggle against enemy radio communications was waged by almost all the combatants. At the beginning of the war, the forms that were most widely developed were the monitoring of the operations of radio means, and the interception of radio transmissions. Jamming, for the purpose of interfering with the radio communications in the armies of the combatant countries, occurred very rarely.

An important role in monitoring headquarters and troops was played by short-wave radio direction-finders that were created during World War I by Russian engineers N. D. Papaleksi and A. L. Mandel'shtam. With the aid of the radio direction-finders it became possible to determine the directions to the emitting radio sets and

to triangulate their location. According to the number of operating radio sets, it was possible to deduce the area where enemy headquarters and troop groupings were located, as well as any changes or relocations. Together with the intercepting of radio messages, it was possible to determine the intentions of the troops, the sectors in which the basic efforts would be concentrated, etc. In 1915 the armies of almost all the combatant states, including Russia¹, had special radio-intelligence services, which were equipped with radio-intercept equipment and radio direction-finders.

[Omission]

Years Between the Wars²

During the years up to World War II, the development of methods for waging the struggle against radioelectronic means followed the course of intensifying the radio-intelligence effort, radio deception, and radioelectronic suppression. Radio-intelligence derives information only from intercepting radio messages and fixing the location of active radio sets with the aid of radio direction-finders. Therefore, if broadcasts of false information are organized, then it is possible to mislead the enemy and force him to take actions which will be beneficial for friendly forces. Thus, a second element in the radioelectronic struggle appeared -- radio deception.

In the Red Army, great importance was attached to problems of deception with the aid of radioelectronic means, and in a number of instances, it resulted in major operational successes. For example, Marshal of the Soviet Union G. K. Zhukov discussed this matter in

¹[For a Soviet view of Russian naval SIGINT in World War I, see "COMINT in the Russian Navy, WWI," *CRYPTOLOG*, May 1976. According to a former Soviet Communications Service chief, Marshal I. T. Peresypkin, from mid-1915 to early 1916, Russian Army radio-intelligence groups were established under the control of army radio-battalion commanders, who were the senior radiotelegraphists. Each group, located at Army Headquarters, was divided into two sections: one section monitored enemy radio stations, while the other engaged in radio intercept. I. T. Peresypkin, *Voennaya radio-svyaz'* (Military Radio Communications), Moscow, Voenizdat, 1962, p. 56. T.R.H.]

²[Peresypkin points out that, during the Russian civil war, some of the reversals suffered by the Communists were due to poor COMSEC on their part. In a similar vein, during the Russo-Polish War of 1920, according to Peresypkin, a Polish General Staff officer stated that Polish COMINT units gained enormous amounts of information because of poor radio discipline on the part of the Russians. Peresypkin, *op. cit.*, pp. 108-110. T.R.H.]

UNCLASSIFIED

his book *Vospominaniya i razmyshleniya* (Recollections and Reminiscences). In 1939, in the combat actions against the Japanese usurpers at Khalkhin-Gol, the command element of the Soviet forces considered the decisive factor of success in the offensive to have been operational-tactical surprise. "For purposes of deception, and maintaining the utmost secrecy concerning our measures, the Military Council of the Army Group, simultaneously with the plan for the impending operation, developed a plan for operational-tactical deception. . . We knew that the enemy was conducting radio-intelligence and was monitoring our telephone conversations. So, for purposes of misinformation, we worked out an entire program of radio and telephone messages. The conversations concerned only the construction of defensive positions and preparations for the autumn-winter campaign. The radio deception was based chiefly on a code that was easy to break. . .

"Subsequent events and the entire course of our offensive operation showed that the special measures of misinformation and deception, as well as other measures taken in preparation for the surprise operation, played a very important role and the enemy was actually caught unawares."³

World War II

During World War II, radioelectronic warfare was further developed and perfected. It was waged by the armies of all the combatant countries. At such time, wide use was made on the fronts of all three components of the radioelectronic struggle: radio-intelligence and radioelectronic intelligence, radio deception, and radioelectronic suppression.⁴

Radioelectronic suppression was the most important and most effective part of the struggle, inasmuch as, by simply creating special suppressing emanations of electromagnetic energy, it was possible to disrupt the operation of the enemy's radioelectronic systems and means. For the first time in history, the Soviet Army used a combination of all three methods of the radioelectronic struggle in the Battle of Stalingrad.

³G. K. Zhukov, *Vospominaniya i razmyshleniya*, Moscow, 1969, pp. 161-163.

⁴[There is strong, but inconclusive, evidence that, in addition to his regular communications duties, Marshal Peresypkin also controlled Soviet military SIGINT activities throughout WWII. For example, see Heinz Hohne, *Codeword: Direktor*, (New York, Coward, McCann & Geoghegan, 1971, p. 37). Hohne cites a publication of the Institute for the Study of the USSR, *Prominent Persons in the USSR* (Munich, April 1960), as his source that Peresypkin was in charge of military intelligence in addition to his position on the Communications Directorate of the General Staff from the summer of 1941 until 1945. T.R.H.]

In November-December 1942, the forces on the Southwest, Don, and Stalingrad Fronts intensified their use of radio intelligence. After encircling the German fascists' 6th Field Army, the command element of the Stalingrad Front created an electronic jamming group in order to suppress the German radio communications. This group had several powerful radio sets. In order to derive intelligence from the radio means of the encircled troops, to direct jamming operations against them, and to determine the effectiveness of suppression, the 394th Independent Radio Battalion was activated. Simultaneously, a special radio set was assigned to deceive the 6th Army Headquarters by operating with the callsigns used by the headquarters of Mannstein's group of forces, which was attempting to break through the encirclement. That radio set received from the 6th Army Headquarters 86 very important radio messages. The operation of the enemy radio sets was suppressed by tuning our radio sets to the frequencies used by the enemy radio sets and conducting "meaningless" transmissions when they started to transmit. The established control over the degree of suppressing the radio communications, as well as the testimony of captured generals and officers of the 6th Field Army, attest to the exceptional effectiveness of the measures that were carried out.

A qualitative leap forward in the development of radioelectronic suppression as the basic method in the struggle against the enemy's radio communications occurred in the Soviet Army in 1943. On 17 December 1942, General Headquarters of the Supreme High Command decided to create special radio-jamming units. Two special-purpose radio battalions were immediately created: the 131st and the 132nd. In 1943 and 1944, the 129th and 130th Radio Battalions were formed, respectively.

These were the first units set up for radioelectronic suppression. The creation of these units was necessitated by the waging of the constant radioelectronic struggle.

All the radio units took the most active part in suppressing the enemy's radio-communications systems and misinforming him. The 131st Radio Battalion operated as part of the Northwestern Front, and the 132nd as part of the Voronezh and Central Fronts (1943); subsequently these units were transferred to the 1st Ukrainian and 2nd Belorussian Fronts.

From 1943 through 1945, the radio battalions suppressed the radio communications of the German fascist forces in the army-corps-division chain of command. These radio units achieved a very high degree of success in suppressing the radio communications of the encircled groupings. The radio battalions set up a complete radio barricade against the enemy's troops. For example, from 23 June through 31 July 1944, the 131st Radio Battalion participated in the Belorussian operation during the encirclement and annihilation of groupings in the Vitebsk area

UNCLASSIFIED

and to the southeast of Minsk. This radio battalion worked round the clock, disrupting 522 urgent and 1665 routine enemy radio messages.⁵ Subsequently, this same radio battalion was given the task of completely suppressing the radio communications of the encircled Koenigsberg garrison, and, most important, of preventing its command element from communicating with Hitler's headquarters. The battalion was very successful in fulfilling this assignment. During a 24-hour period in the assault on Koenigsberg, the main radio transmitter of the encircled garrison attempted to switch to 43 different frequencies, and every one of the frequencies was suppressed. The corps and division radio communications of the defending troops were also completely suppressed. Then the main radio transmitter began transmitting in the clear the garrison commander's order concerning the capitulation of the troops.⁶ The commander of the Koenigsberg garrison forces, General-Colonel Lasch, said at his interrogation, "As a result of the terrible artillery softening-up, the landline communications in the fortress were put out of commission. I had hoped to maintain radio communications with Courland, the Zemland group, and Central Germany. However, the effective jamming measures used by the Russians prevented the transmission of radio messages and my operations could not be coordinated with the headquarters of the Supreme High Command. That was one of the reasons for my capitulation."

The 132nd Radio Battalion also operated just as effectively. In March 1945 the troops of the 1st Ukrainian Front waged combat actions to annihilate the encircled garrisons in Glogau and Breslau. The 132nd Radio Battalion, having divided its forces and equipment into two groups, successfully suppressed the radio communications of those garrisons. During a 15-day period (from 5 through 20 March 1945) the 132nd Radio Battalion disrupted 358 radio transmissions in the Glogau area, 735 in the Breslau area, and prevented 2801 other attempts to establish contact.⁷

Later on, the battalion's main forces and equipment were directed at suppressing the radio communications between the headquarters of the encircled 5th Army Corps and the 9th Field Army headquarters.⁸

In addition to the special radio units, in the course of the Great Patriotic War, the standard equipment issued to troops was often used for the purpose of suppressing the enemy's

⁵Archives of the USSR Ministry of Defense, collection 131, list 36683, folder 1, sheet 9.

⁶Ibid., folder 1, sheet 17.

⁷Archives of the USSR Ministry of Defense, collection 132, list 328334, folder 1, sheet 31.

⁸Ibid., sheet 32.

radio communications. For example, in February 1944, during the encirclement of the German fascist forces in the Korsun'-Shevchenkovskij operation, the headquarters of the 27th Army received intercepted radio messages which were being exchanged between the commanders of the encircled troops and the commanders of the troops outside the ring of encirclement. The command element of the 27th Army decided one night to prepare all the powerful troop radio transmitters to suppress the radio communications of the encircled forces. When the enemy began to attack, we succeeded in completely suppressing his radio communications, thus making it impossible for the encircled grouping to coordinate their actions in breaking through the ring of encirclement.

Thus, during the course of the Great Patriotic War, the struggle against the enemy's electronic systems by means of intelligence, jamming with special emanations, and radio deception found its further development in the Soviet Army. In disrupting the work of radio communications, wide use was made not only of special units created for this purpose for the first time, but also the troop radio means.

[Omission]

Thus, electronic warfare was further developed and improved during World War II. The scope of application of the means of radio-electronic suppression increased; special units (subdivisions) began to be created; and the tactics for their application began to be developed.

Postwar Period

In the postwar period, imperialism has unleashed many wars and armed conflicts. Experience shows that in each of them, means of electronic warfare were used. They were used for resolving not only strategic tasks, but also operational-tactical ones.

Simultaneously, the armed forces of all the technologically developed countries began to develop a fourth element in electronic warfare: protecting the electronic means of friendly troops from the intelligence-gathering and jamming operations conducted against them by the enemy.

At the present time, electronic warfare is undergoing a new phase in its stormy development. As events have shown, not a single combat engagement, not a single operation by any branch of the armed forces, can begin or can be carried out without the broad use of the forces and means of electronic warfare.

[redacted] has prepared an Annotated Bibliography of open-source materials in Russian which deal with SIGINT and EW. To obtain a copy of the bibliography, write or call: PI, CRYPTOLOG Editor, 5642s.

P.L. 86-36

(UNCLASSIFIED)

UNCLASSIFIED

~~CONFIDENTIAL~~**ANOTHER WORD ON AG-22**

Fifteen years ago, an intercept operator copied a radio signal onto six-ply paper. He copied while the case was active and usually went back and put in comments when the case went down or paused. The comments appeared not at the place where the pause occurred but at the place where they were relevant. If the operator discovered 5 minutes into the copy that he was hearing a letter wrong, he could go back and correct all the occurrences of the letter -- or simply tell the traffic analyst, who was colocated with the intercept operator.

The traffic analyst, at the intercept site, could analyze the traffic in detail -- at a leisurely pace -- and could inform the intercept operator immediately of his conclusions. He could even consult with the intercept operator to help determine what was going on in the traffic.

The traffic analyst at the intercept site was an important factor in intercept quality. His close contact with the intercept operator speeded up the training of "jeep" intercept operators and also contributed to trained operators' morale and motivation by continually keeping them informed of what was happening. The better intercept operators always had a great interest in analytic details of their targets.

Gold-flow problems caused NSA to look for ways to reduce overseas manning. At first, the technology was not available to move the intercept operator back to the States, but it must have seemed a simple matter to move traffic analysts back. Why, they could analyze traffic at NSA just as easily as at the intercept site, couldn't they? AG-22 would give the traffic analyst his traffic on a real-time basis at NSA.

Budget problems caused NSA not just to move those traffic analysts back, but to eliminate them altogether. There was a set of traffic analysts already at NSA and why did we need duplicative traffic analysis?

The problem is this: those two sets of traffic analysts were not doing duplicate work. The analyst at NSA was performing long-range analysis, building on the short-term work done in the field. The analyst in the field was providing a needed service in short-term analysis and in intercept quality control and in intercept operator training and in intercept operator motivation.

Can AG-22 or any other computer system do that? I think not.

~~(CONFIDENTIAL)~~

(UNCLASSIFIED)

A VEXING AGENCY-WIDE PROBLEM

Frederic O. Mason, Jr.
P11 ? ?



For the past several months a problem has both interfered with and frustrated the best efforts of our analysts. Happily, it has now been solved, but it required a new concept in collection and a bit of special reporting not included in the routine TECSUM.

The problem was complicated by a lack of funds with which to increase the volume of co-ordinated data collected, and by unverified reports of items collected elsewhere.

Each item collected provided an example of a term which fell clearly into either an "A" or a "B" configuration, but there were also several occurrences of a "C" and one example of a "D" configuration. Also, collateral reports included references of configurations which could not be any of these (arbitrarily designated "X," until examples are in hand). Normal collection was on a very small scale at first, with many items collected but not reported.

It became clear, even before systematic dual collection was attempted, that the system relied on rotors of different sizes, all stepping at the same time, but the resultant sequence could not be reconstructed from unrelated intercepts.

(Continued, next page)~~CONFIDENTIAL~~

Recently it became possible to coordinate two collectors so that sequential items from the same series became available. With no more than ten such paired items, together with previously collected data, it became possible to reconstruct the rotors and to establish the entire "A" and "B" sequences. Further, it became clear that the "C" and "D" sequences were based on permutations of the "A/B" rotors, although it has not been possible, with present collectors, to accumulate enough data to reconstruct the "C/D" sequence.

The final problem -- that of understanding the conditions under which the A/B, or the C/D, sequences are used -- was solved when data not previously required was added to the TECSUM.

The solution required that two cups be collected sequentially, using one or two operators, from the same vending machine, and that the Poker Fun cups ("For Consumer Amusement Only -- Use for Gambling or Awarding Prizes May Be Unlawful") be marked in the order received. And the final problem required that a distinction be made between hot cups (the A/B set) and cold cups (the C/D set). A cup from the A set is distinguished by having cards, red or black, in BRRBR order, and is always followed by a cup from the B set, which has cards in BBRBR order and is always followed by a cup from the A set. Both A and B end in suits ♦♣♦, which is a reversal of the C and D final cards ♦♣♦.

We now know the full A/B sequence and have devised a handy-dandy chart which will let us predict, from any one cup, what poker hand will appear on the next cup.

As for rotors, each card position in each set has three, four, five, or seven cards, which repeat in order. Rotors would give this effect.

However, our collectors don't normally collect C/D cups, and reports of flushes (not possible with either A/B or C/D sets) remain unconfirmed. Solutions to these remaining, and vexing, problems must wait for other analytic groups to solve.

Meanwhile, here are sample data (you can collect more if you wish), which are sufficient to a solution. The first cup we collected, arbitrarily designated as at position A001 in the sequence, was the hand 10♦ 8♦ 10♥ 2♠ K♦.

We also collected samples of various winning hands, as follows:

4 of a kind

10♣ 8♦ 10♥ 10♠ 10♦
K♣ 9♣ K♥ K♣ K♦

Full house

K♣ 9♣ 9♥ K♣ K♦
K♣ 9♣ K♥ 9♣ K♦

3 of a kind

7♣	8♣	K♥	K♠	K♦
8♣	K♣	K♦	S♣	K♥
9♣	A♣	A♦	K♣	A♦
10♣	9♦	Q♥	Q♣	Q♦
A♣	7♥	A♥	K♣	A♦
A♣	7♥	A♥	A♣	K♦
A♣	9♦	Q♥	Q♣	Q♦

Straight

7♣	8♣	9♥	10♣	J♦
7♣	8♣	9♥	J♣	10♦
8♣	7♦	10♦	J♣	9♥
J♣	8♣	9♥	Q♣	10♦
K♣	9♣	J♥	10♣	Q♦

2 pairs

J♣	8♣	2♥	2♦	J♦
J♣	8♣	K♥	J♣	K♦
K♣	9♣	2♥	9♣	K♦

1 pair

7♣	8♣	J♥	Q♣	J♦
10♣	7♥	A♥	A♣	J♦
A♣	2♦	8♥	9♣	A♦
A♣	7♥	A♥	K♣	Q♦

The following pairs have been artificially constructed from the answer, since the analysts, in an unfortunate excess of parochialism, attempted to frustrate competition for the solution by destroying their data. However, the answer has been checked repeatedly at the point of intercept and these data are thereby validated, even if they cannot be retrieved from the data base we hang on our wall.

First member of pair

Followed by

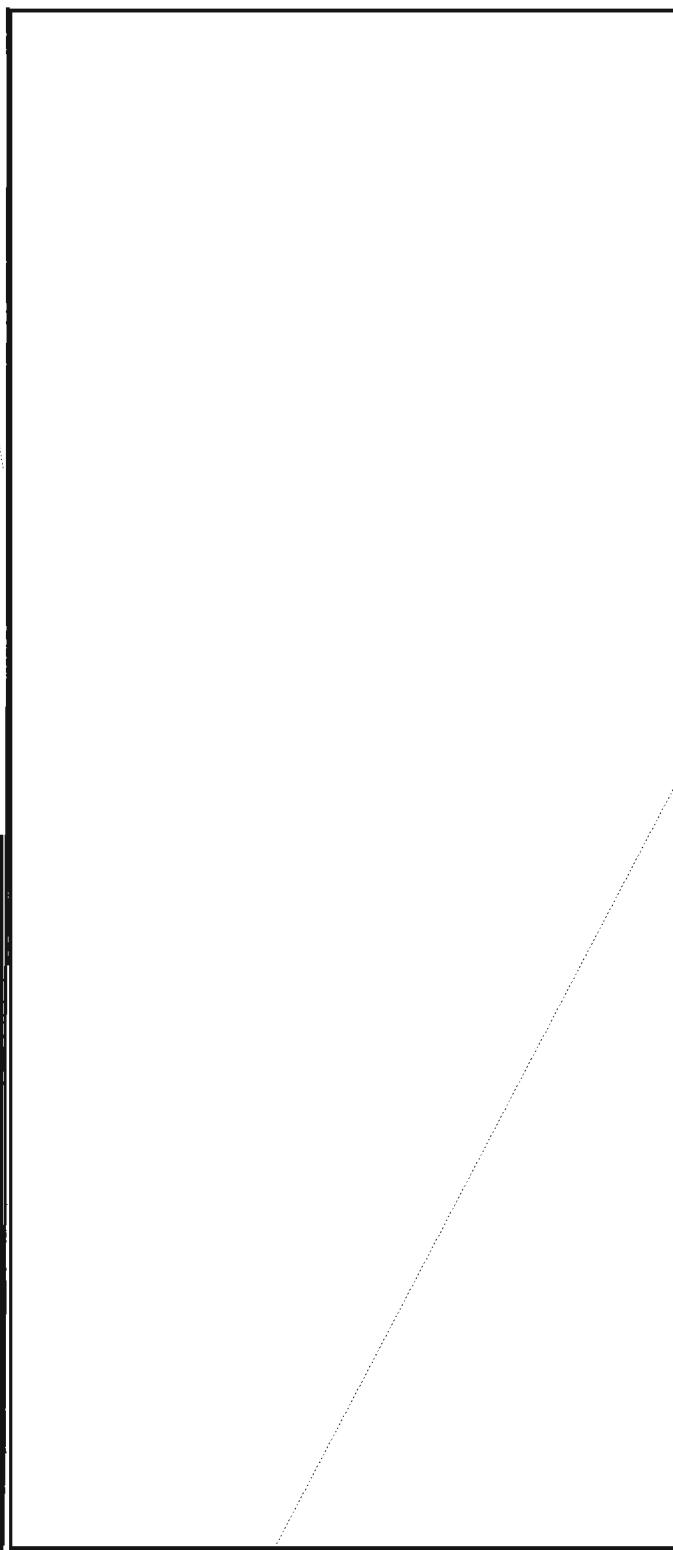
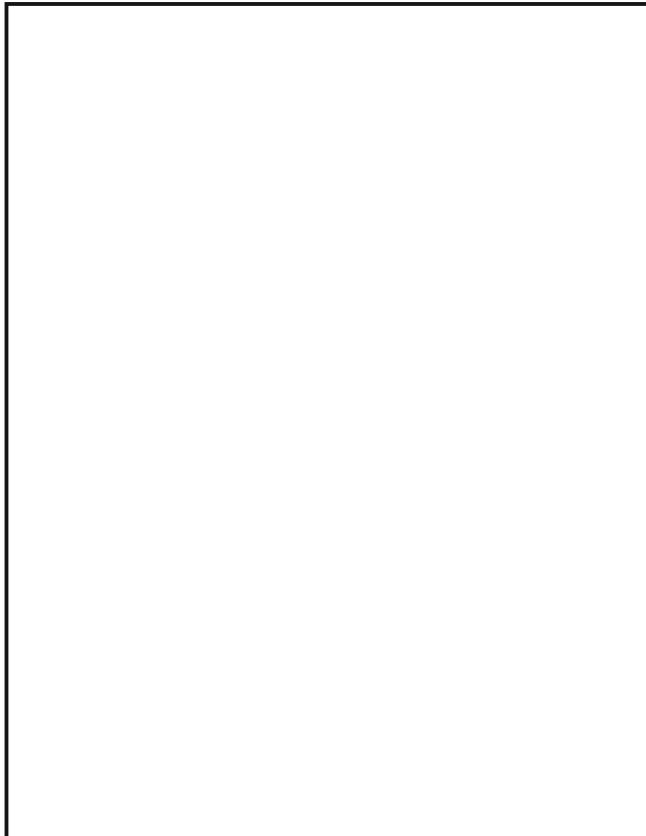
10♣	2♦	8♥	K♣	10♦	7♣	8♣	9♥	A♣	J♦
J♣	8♣	K♥	2♣	Q♦	10♣	9♦	Q♥	J♣	K♦
A♣	8♦	10♥	9♣	J♦	J♣	8♣	2♥	10♣	A♦
7♣	8♣	K♥	J♣	J♦	Q♣	9♦	Q♥	Q♣	A♦
K♣	9♣	K♥	9♣	K♦	A♣	9♦	Q♥	10♣	10♦
Q♣	8♦	10♥	J♣	10♦	K♣	9♣	2♥	Q♣	J♦
10♣	7♥	A♥	10♣	K♦	7♣	8♣	K♥	K♣	10♦
7♣	8♣	9♥	A♣	J♦	Q♣	8♦	10♥	2♦	A♦
A♣	9♦	Q♥	2♣	K♦	J♣	8♣	J♥	J♣	10♦
K♣	9♣	2♥	Q♣	K♦	A♣	7♥	A♥	9♣	10♦
7♣	8♣	J♥	K♣	A♦	Q♣	2♦	8♥	A♣	Q♦

The problem for you -- and the author will buy one cup of coffee for the first correct answer -- is to provide the sequence position of the only cup having four aces.

(Solution next month)

~~SECRET SPOKE~~

MORE THOUGHTS ON "QUESTIONABLE" SIGINT



LANGUAGE SKILL FILE

The following article appeared originally in Field Information Letter, June 1976. It has been slightly revised and updated by the authors.

Producing an accurate inventory of the Agency's linguistic resources has become a major management concern in recent years. In this context, the term "resources" encompasses assets, versatility, and quality. While it has been possible to assess language requirements with a fair degree of accuracy by using the billet requirements expressed in the Table of Distribution (TD), attempts to assess capability have been frustrated by the lack of verifiable data concerning incumbents of those billets. Frequently, supervisors' evaluations, or even self-evaluations, have been relied upon in determining skill level. Taking inventories has also been complicated by the fact that some people with a language proficiency are no longer working in the language career field and some linguists have a proficiency in a number of languages, even though they may be using only one in their current position.

After analyzing the problem it was concluded that the managerial tools now available -- including the TD, certification statistics, and language proficiency test (LPT) results -- could not be relied upon to give an accurate inventory. We also concluded that an accurate picture of the linguistic capability of the work force would be gained if a language skill level was associated with an individual, rather than a billet or Career Occupational Specialty Code (COSC). As a result, a Personal Skill Code (PSC) was established and is now being used to identify the linguist skills of all Agency personnel regardless of the job title they may currently hold. The skill code has four basic elements that indicate: 1) skill level; 2) language digraph; 3) method by which the level was verified; and 4) year the level was verified. Additional elements can be added to these to indicate a voice-analysis capability.

To date, codes have been assigned to all civilians whose background reflects language training; everyone coded at the zero ~~to one~~ 4. (c) level has been encouraged to be tested in 86-36 those languages.

Using the skill codes and the Personnel Information Distribution System (PIDS) it is possible to retrieve language data on-line by language digraph, skill level, and organization. It is anticipated that this information could be particularly useful during crisis situations.

[REDACTED] the people coded at the zero and one levels might be of greater interest for retraining or for receiving additional training. The system printout, in response to these requests, would give each person's name, grade, COSC, and the last two positions of his job number (which indicate the language he/she is currently using, if any) and his/her skill code.

The system also allows managers to make use of the versatility of their work force. On a day-to-day basis a manager may only be interested in the fact that an employee has a proficiency in the language of the primary target he is working on; however, secondary language skills could be of significance in areas where there is an occasional requirement for someone with training in other languages or where there have been shifts in the emphasis placed on individual targets. Similarly, languages for which there is no operational requirement, or a very small requirement, are of interest largely because of the information provided on an employee's capa-

bility to learn a language in a particular family of languages. EO 1.4. (c)
P.L. 86-36

The Personal Skill Code is still in a developmental stage and will be modified in future months to identify individuals who have not yet achieved certification but have passed one or more parts of the PQE and to identify individuals who have the capability to work with voice as well as written language materials. Guidance from the Language Advisory Committee will be sought in determining when a language proficiency might be considered dormant and when it should be thought of as beyond revitalization.

A summary of the language skills currently represented in the field for individuals coded to date is given in the following table. If you are interested in obtaining a copy of the *Guide to the Language Skill File*, which gives examples of the output that can be obtained by using each of the programmed segments in the PIDS, or if you have questions on the use of the file, contact M33 (8267 or 8276).

SUMMARY OF LANGUAGE SKILLS REPRESENTED IN F (Field Units)

Language	Level	Code
Arabic	0	AR0
Arabic	1	AR1
Chinese	0	CH0
Chinese	1	CH1
French	0	FR0
French	1	FR1
German	0	GE0
German	1	GE1
Italian	0	IT0
Italian	1	IT1
Japanese	0	JA0
Japanese	1	JA1
Korean	0	KR0
Korean	1	KR1
Mandarin	0	MA0
Mandarin	1	MA1
Persian	0	PE0
Persian	1	PE1
Russian	0	RU0
Russian	1	RU1
Spanish	0	SP0
Spanish	1	SP1
Turkish	0	TR0
Turkish	1	TR1
Vietnamese	0	VI0
Vietnamese	1	VI1

NSA-CROSTIC No. 5

By A. J. S.

The quotation on the next page was taken from a published work of an NSA-er. The first letters of the WORDS spell out the author's name and the title of the work.

P.L. 86-36

DEFINITIONSWORDS

UNCLASSIFIED

UNCLASSIFIED

A Technical Journal, Summer 1967
CAMINO
BY DORIS MILLER AND [REDACTED]

CRYPTOLOG, July 1975

iCAMINO EN INGLÉS!
ronic War

SOME IDEAS ABOUT MECHANIZED LANGUAGE WORKING AIDS

no emergency
are wrong.
nitive, and urgent
endangers a

ceeding steps
a speed also merely
with four million me...
increase that to fort...
with tempo of
better.

PRO

CRYPTOLOG, February-March 1975
CAMINO NEWS

This brief paper is intended to present some general comments covering my experience with the CAMINO Natural-Language Machine Files and other computerized natural-language working aids. It has seemed to me that these remarks might be of some value or interest to others concerned with mechanized language aids, whether as users or as designers.

In considering the design of a natural-language dictionary (as in any data management system, however sophisticated or rudimentary), there are three obvious kinds of things that need to be done:

- a) building the file from external sources;
- b) maintaining the file by additions, deletions, and corrections; and
- c) querying, displaying, or extracting data from the file for day-to-day operational use.

The attention of most computer specialists has centered on the tasks under heading c: the ways of looking up, rearranging, manipulating, and displaying data from an existing file. This is, admittedly, the most interesting area conceptually, and provides the most scope for inventiveness in software design and programming techniques.

Unfortunately, however, at least in my experience, the real problems involved in the design of natural-language working aids revolve around areas a and b, and especially area a: the initial building of the glossary file. The querying or displaying of data from a completed file has rarely presented any problems in the CAMINO files or any other mechanized working aids I have worked with.

~~CONFIDENTIAL~~EO 1.4. (c)
P.L. 86-36

In maintaining the file once it has been established and has completed its initial rapid growth, the file sponsor must see to it that the file continues to be responsive to all his users and their needs, in spite of frequent reorganizations of Agency personnel, changes in missions, and new developments in the external world of international events. He must make a continuing effort to collect contributions of new terms, and solicit constant feedback from all file users, while searching for new sources of data that should be added to the file.

Now let's shift our attention to the question of how the tasks outlined above can best be accomplished at present and in the near future and why. To most computer-oriented managers, it seems obvious to the point of triviality that each sponsor who needs a mechanized language aid should do all the work himself, preferably at "a terminal" (unspecified). If he cannot do all the work himself, for whatever reason, he should get "somebody else" (also unspecified) in his own organization to do it for him. The hypothetical manager we are quoting sees no difficulty in any of this, and considers the problem solved by his advice.

In certain specific contexts, where on-line terminals have already (for a variety of historical or practical reasons) become the primary or only way of accessing and manipulating all data for a problem, it makes excellent sense to put language aids on line too. In these cases

[redacted] the needs of one specific set of users are being amply met by a complete system design that includes all the working aids they require. There are still, however, many scattered users who are, and may remain for some time, outside of these advanced projects. For them a generalized or standardized conventional file-maintenance procedure, involving periodic updating and reissue of printouts, has been an effective and economical way of getting the job done.

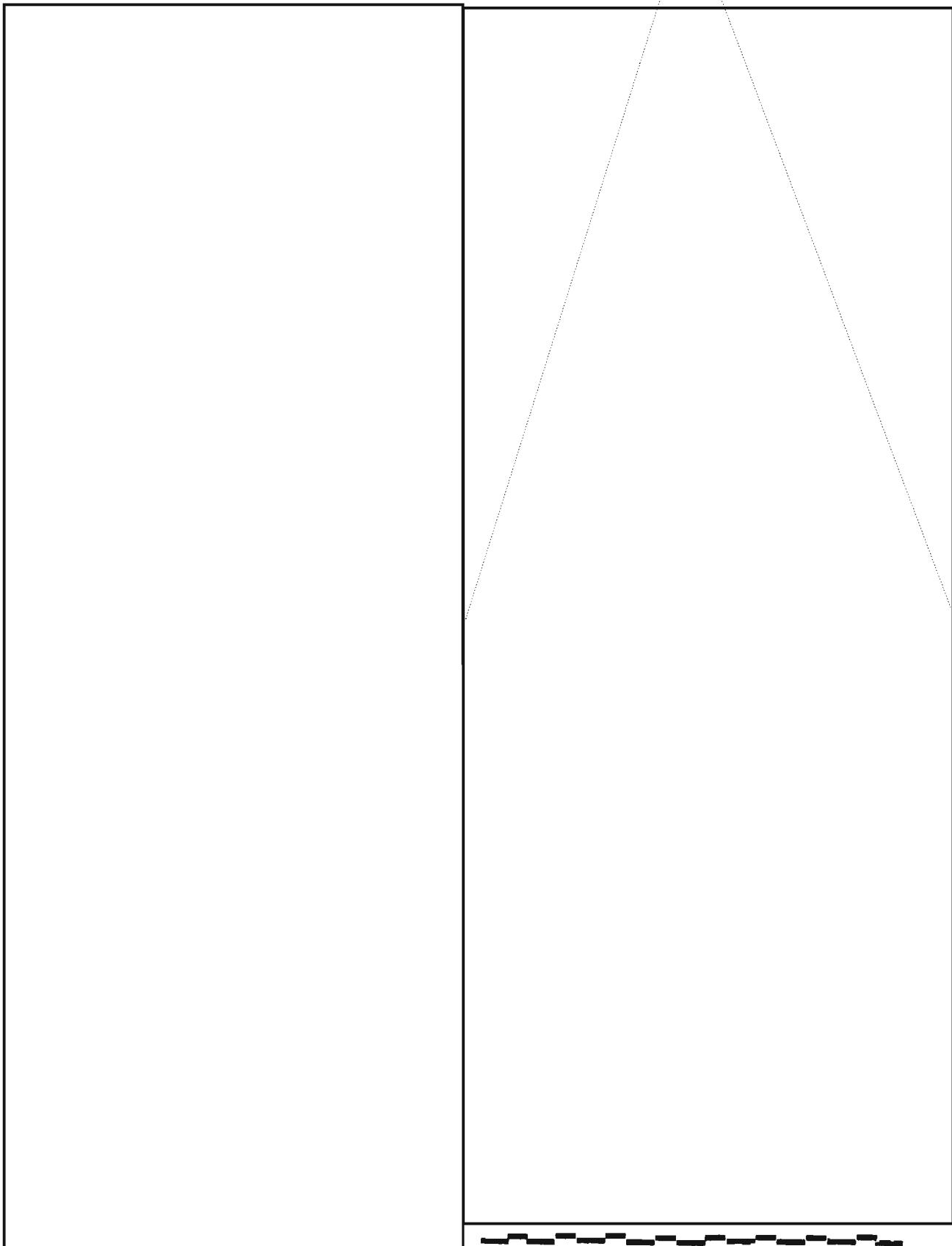
Faced with all these immediate pressures, the senior linguist has little or no time, energy, or peace of mind left over to work on the dictionary at all, let alone do the extra initial work required to mechanize it. He certainly is not usually able to spend hours of his time sitting at a terminal (which he is not routinely using for any other purpose), keying in his own data or making line-by-line changes. Finding someone else to do these things within his own organization is also apt to be very difficult in practice. Everyone else who is qualified is just as busy, and just as unable to take time to sit at a console for hours on end, concentrating on the dictionary. Helpers who are not qualified almost invariably cause far more problems than they solve.

Our hypothetical manager, whom we have been quoting as a Devil's advocate, has an immediate reply, by which he again seeks to define away the awkward resource-allocation problem: "If the sponsor organization doesn't need the dictionary badly enough to assign the necessary resources to it, obviously it isn't really needed at all, so we can forget it." Again, I cannot accept this representation of the situation, however useful it may be in simplifying matters for the manager.

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

EO 1.4. (c)
P.L. 86-36



.....

October 76 * CRYPTOLOG * Page 14

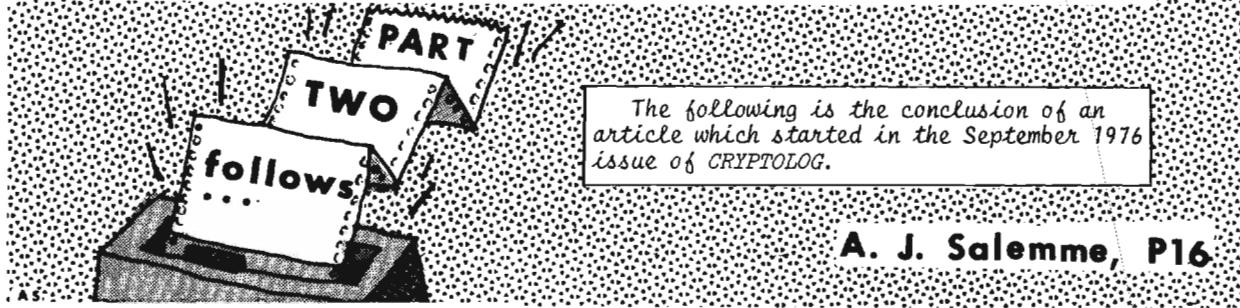
~~CONFIDENTIAL~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET UMBRA~~

EO 1.4. (c)
P.L. 86-36

MACHINE-PRODUCED AIDS FOR THE LINGUIST



The following is the conclusion of an article which started in the September 1976 issue of CRYPTOLOG.

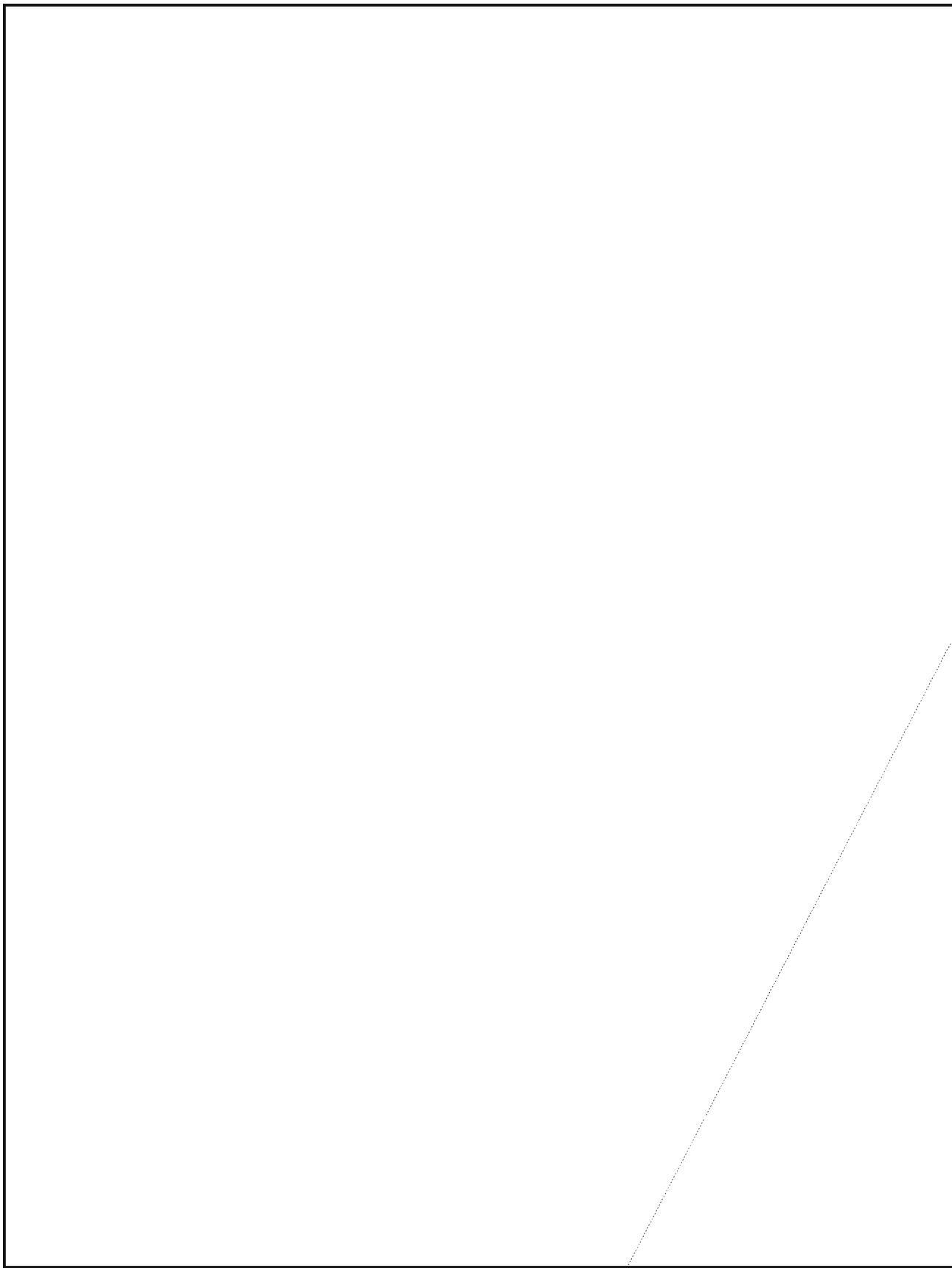
A. J. Salemme, P16

October 76 * CRYPTOLOG * Page 16

~~TOP SECRET UMBRA~~

EO 1.4. (c)
P.L. 86-36

~~TOP SECRET UMBRA~~



October 76 * CRYPTOLOG * Page 17

~~TOP SECRET UMBRA~~

EO 1.4. (c)
P.L. 86-36

October 76 * CRYPTOLOG * Page 18

~~TOP SECRET UMBRA~~

EO 1.4.(c)
P.L. 86-36

~~TOP SECRET UMBRA~~

```
#00222001..z450  
#00222002..z117  
#00222003..z578  
#00222004..z98..z1  
#00222001..z445  
#00222002..z519  
#00222003..z58..z1  
#00222003..z85..z1  
#00222002..z383  
#00222001..z183  
#00222002..z562  
#00222001..z62  
#00222001..z441  
#00222002..z171  
#00222001..z574  
#00222001..z456  
#00222002..z117  
#00222003..z578  
#00222004..z98..z1  
#00222001..z445  
#00222002..z519  
#00222003..z58..z1  
#00222003..z85..z1  
#00222002..z383  
#00222001..z183  
#00222002..z562  
#00222001..z62  
#00222001..z441  
#00222002..z171  
#00222001..z574  
#00222001..z456
```

Classic Use of Computers: Research in Greek

Research in the classics that once took months or even years can now be accomplished in minutes with the help of a computerized data bank of the classical Greek language. Eventually the system will store 90 million words to form the first thesaurus of the language.

The ability of the computer system to provide basic research mate-

rial quickly and efficiently frees the scholar of the task and allows him to devote more time to analytical work, according to Prof. Theodore Brunner, director of the Thesaurus Linguae Graecae project at the University of California at Irvine.

The traditional method of accumulating information about a specific author's writing, or all the writings of a given period, would

involve scholars locating and reading texts, analyzing word use, recording each word with its sentence context on a separate index card and filing the cards alphabetically. The process is usually long and tedious, according to Dr. Brunner.

With the Irvine system, Greek texts are key-punched and recorded on magnetic tapes in a special code. The tapes are scanned by computers.

programmed to store and process the information into word use and meaning. The computers can retrieve specific material and provide printouts in both Greek and English which scholars can use for compiling lexicons and key-word-in-context concordances.

Dr. Brunner says the computer requires about two minutes to find all the uses of a given word in the half-million words of Plato's writings. The old method would take a scholar several years to do the same research, Dr. Brunner says.

So far the project, begun in 1972, has entered 18.5 million Greek words on tape, and the data bank is being used by scholars in such fields as literature, philology, linguistics, history and philosophy.

New York Times,
5 April 1976

(UNCLASSIFIED)

~~SECRET~~

(UNCLASSIFIED)

To the Editor, CRYPTOLOG:

[redacted] article, "Integrated Analysts for Asia: A Cohesive Approach" (CRYPTOLOG, August 1976), virtually admits to sex discrimination in the placement of integrated analysts. While I am perfectly willing to admit to the desirability of "empathy toward the Asian attitude," I am also only too well aware of the large number of women whose lack of promotion has been explained by "but the male candidate has had an overseas tour." Does B Group need reminding that Agency policy forbids them to deny women desirable overseas positions on the basis of sex? I think [redacted] owes CRYPTOLOG readers an explanation.

"Firebrand"

P.S. I'm surprised you let him print that!

Editor's reply:

P.L. 86-36

The Publisher and Editorial Board very rarely advise an author to modify his or her statements on the basis of inappropriateness. We feel that, inasmuch as the views expressed in each article are the author's own (and do not have to be "coordinated" or "cleared" with anyone else at any level, unless the author so desires), every author has the right to express his or her technical opinion, however controversial (or even however half-baked) it might seem to be. It is not true, as people sometimes say around the CRYPTOLOG office, that "CRYPTOLOG will print anything!" CRYPTOLOG will print anything that has operational relevance. If any reader disagrees with the author's views, that reader is welcome to contribute a counterview (anonymously, if desired), and that counterview will be printed, so long as it contains a valid statement, rather than just *ad-hominem* (should we also include *ad-feminam*?) invective. So, in effect, I'm surprised that you're surprised that CRYPTOLOG "let him" print it.

*Ed.**Speaking of "his or her" . . .*

To the Editor, CRYPTOLOG:

I have admired the style of CRYPTOLOG since the first issue. The quality of the English therein has been a delight to its readers and an example to all of us who write. But I must protest the use of two particular pronouns in one recent article.

Is the use of "he/she" and "his/her" to refer to a [redacted] operator really necessary? It seems to me that it condescends. It is a repeated reminder of something we accept -- the

[redacted] USAF,
[redacted]

(SECRET CCO)

~~SECRET~~

UNCLASSIFIED

operator might be a man or a woman. Those who do not accept this will certainly not be influenced by seeing these words in print. In fact, these readers will probably be far more annoyed than I am.

If such usage is required by agency or governmental guidelines, then I am alarmed. If not, then let us revert to the use of masculine pronouns to refer to a person of unspecified gender.

G43

Editor's reply:

As far as I know, there are no such agency or governmental guidelines. As far as CRYPTOLOG editorial policy is concerned, we do not add "or her" unless the author himself or herself includes those words in his (need I add "or her"?) article. Personally, I feel that excessive use of "his or her" draws the reader's attention away from what is being said to how it is being said. I would hope that most CRYPTOLOG readers do read the magazine for what its authors can communicate to them. Unfortunately, the English language itself is flawed. People can suggest all-purpose pronouns that refer to either males or females, but that doesn't mean that everyone who speaks English will accept them. Even if one uses the graphic convention "s/he," how would one pronounce it? Moreover, the suggested conventions aren't really that all-inclusive anyway. A letter to the editor of *The Wall Street Journal* last year suggested that the all-inclusive pronoun should include not only "he" and "she" but also the third-person inanimate pronoun: it should mean "he or she or it." The writer suggested the word "h'orsh'it." I think he's on the right track.

Ed.
(UNCLASSIFIED)

FIND ANY TYPOS?

Occasionally the only comment the Editor hears about what he thought to be a particularly informative issue of CRYPTOLOG is, "There's a typo on page 13!" Therefore he was pleased to see, in a local Maine-coast newspaper recently, the nice way in which a fellow editor handles the situation.



October 76 * CRYPTOLOG * Page 21



P.L. 86-36

**WORK QUOTAS
FOR SOVIET TRANSLATORS**

G5

Author's note: The following information is derived from an article in *The ATA Chronicle* which, in turn, was extracted from *Scientific and Technical Translations in Soviet Industry*, by I. P. Smirnov.

The All-Union Translation Center for Scientific-Technical Literature and Documentation in Moscow employs approximately 5000 full-time translators and several times that many part-timers. These translators, as all production workers in the Soviet Union, have work quotas to fill. In filling these quotas, the translator must read the manuscript before it is retyped, correct the retyped version, proofread the corrections, and closely scan the corrections made by the scientific editor. No allowance is made for difficulty of the text.

And what are these quotas? Languages are divided into three classes, with a different quota in number of words per month to be translated for each class. The word count is made from the target language (usually Russian) and not from the source language, thus penalizing the translators -- e. g., no definite and indefinite articles in the count.

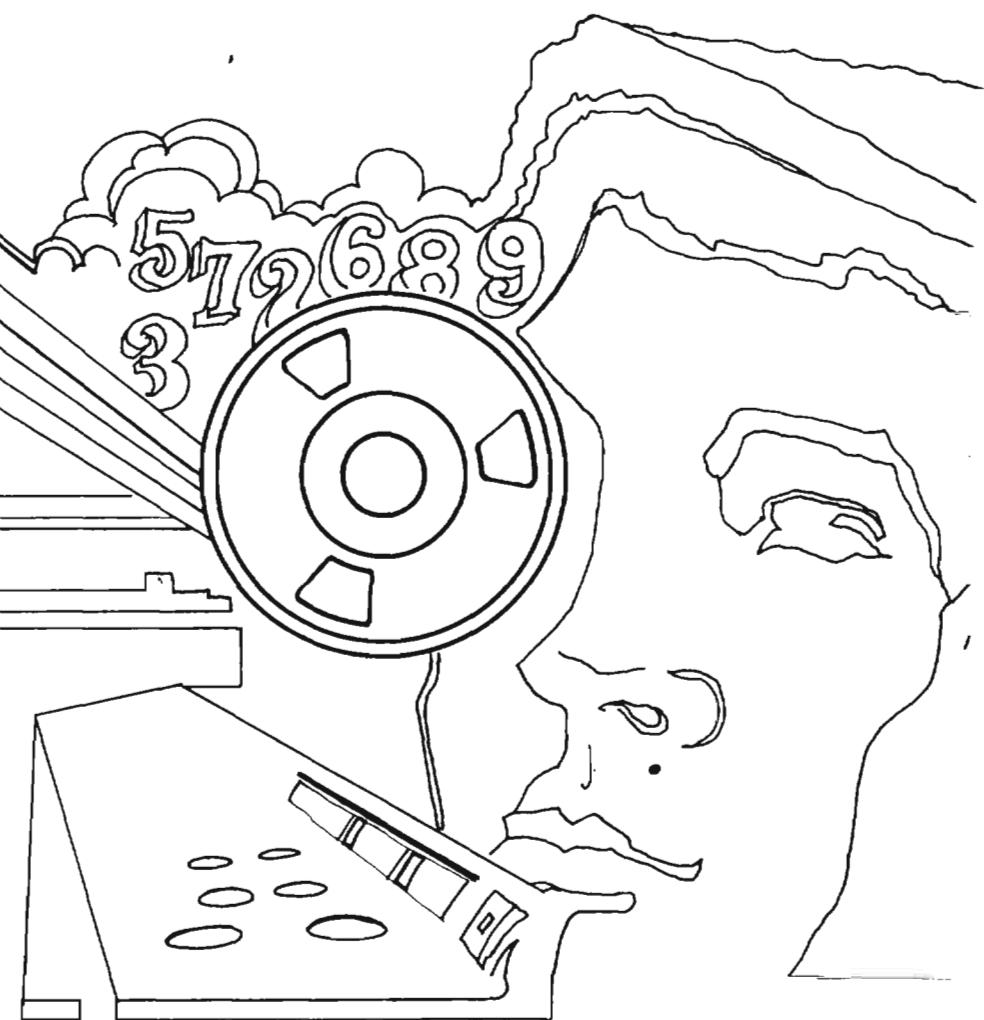
<i>Quota (words per month)</i>	<i>Source language</i>
24,000-32,000	English, German, French, Spanish, Italian, or a Slavic language
16,000-24,000	Hungarian, Finnish, Dutch, Portuguese, Albanian, Greek, Romanian, or a Scandinavian language
14,000-20,000	An Asian language

If the translator dictates -- rather than writes or types -- the translation, the quota is increased by 8000 words. Any volunteers for work norms?

(UNCLASSIFIED)

UNCLASSIFIED

~~TOP SECRET~~



~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~